REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
22-07-2010	Final Report	12 October 2007 - 12-Jun-10

4. TITLE AND SUBTITLE

Information Transfer in Wireless Networks

5a. CONTRACT NUMBER
FA8655-08-1-3018

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Jerzy Konorski

5d. PROJECT NUMBER

5d. TASK NUMBER

5e. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Gdansk University of Technology
ul. Narutowicza 11/12
Gdansk 80-952
Poland

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

EOARD
Unit 4515 BOX 14
APO AE 09421

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
Grant 08-3018

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Ad hoc, mesh, and other unstructured wireless networks are worth studying due to their potential of becoming an alternative, survivable communication infrastructure in case of a major disaster or security breach incapacitating the wired backbone. While the design of effective data transfer mechanisms in wireless networks is maturing, new challenges arise regarding information transfer. This is partly because wireless nodes' increased autonomy and anonymity lead to non-punishable node selfishness. Hence, relative to wired networks, it is no longer clear if a given piece of protocol data carries information - i.e., if it increases a selfish recipient's ability to achieve its objectives. Thus the distinction between data and information is linked to incentive compatibility and nodes' willingness to contribute to the network functionality. At the same time, measuring the amount of information in transferred data becomes vital. Accordingly, the project focused both on game-theoretic and information-theoretic aspects of wireless networks.

15. SUBJECT TERMS
EOARD, Wireless Networks, Information Assurance, Ad-hoc Networks

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18, NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			JAMES LAWTON Ph. D.
UNCLAS	UNCLAS	UNCLAS	UL	13	19b. TELEPHONE NUMBER *(Include area code)* +44 (0)1895 616187

Grant # FA8655-08-1-3018
"Information Transfer in Wireless Networks"

Final Report, July 1, 2010

This material is based upon work supported by the European Office of Aerospace Research and Development, Air Force Office of Scientific Research, Air Force Laboratory, under contract FA8655-08-1-3018 (originally assigned number FA8655-07-1-3071)

Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the European Office of Aerospace Research and Development, Air Force Office of Scientific Research, Air Force Laboratory.

The Contractor, Dr. Jerzy Konorski, hereby declares that, to the best of his knowledge and belief, the technical data delivered herewith under Contract No. FA8655-08-1-3018 is complete, accurate, and complies with all requirements of the contract.

DATE: **July 1, 2010**
Name and Title of Authorized Official: **Dr. Jerzy Konorski**

I certify that there were no subject inventions to declare as defined in FAR 52.227-13, or subcontracts awarded, during the performance of this contract.

DATE: **July 1, 2010**
Name and Title of Authorized Official: **Dr. Jerzy Konorski**

Date started

December 15, 2007

Principal staff

Dr. Jerzy Konorski (Gdansk University of Technology, Poland), PI
Prof. Wojciech Szpankowski (Purdue University, West Lafayette, IN), Consultant

1. Program overview - summary of main points

- The project was registered at Gdansk University of Technology, Faculty of ETI, in December 2007 after preliminary talks and clarifications regarding the (no longer applying) VAT exemption. It was agreed between the Project Manager and the PI that a 22% overhead was being added to the project funding to cover the unexpected VAT expenses. Also, the division of labor between the PI and Consultant was decided.

- Advance payment of $10,000 arrived in April 2008, and the check was cashed on June 13 and deposited in the project's account. That preliminary funding was partly used to cover the liabilities arising from earlier expenses related to the 1st IEEE Conference on Information Technology held at Gdansk University of Technology in May 2008. In view of possible urgent payments of conference fees later in the summer of 2008, the PI and Consultant agreed to postpone remuneration for staff hours pending arrival of further payments.

- In June 2008, to ensure smooth work on the preparation of simulation and lab experiments by the local staff in the early phase of the project, as well as to enable more conference travel related to the project, co-funding was secured at Gdansk University of Technology by appropriation of some funds from a local grant (as acknowledged in some papers cited in the paper list below).

- In winter and spring 2008, local lab equipment at Gdansk University of Technology was reviewed and complemented to create a possibility of emulation of a multihop topology and provide experimental verification of our theoretical findings; it is planned to use financial support from a local grant. In parallel, work was advanced on simulation tools, in particular with a view on a flexible hybrid simulator that could accept traffic from a real wireless network segment.

- In May 2008, further consultation took place involving the PI and Consultant during the visit of the latter to Poland; the main topic was the features of a wireless network performance model to be further entered into the game-theoretic payoff model.

- Partial results of the project were presented at the above mentioned IEEE Conference on Information Technology by the PI and two co-workers participating in the project.

- In August 2008, the second installment of $20,000 was received and the check was cashed in the beginning of September. Part of the incoming funding was used to cover the registration fee of Innovations'08 conference, a December event planned as the last activity of the project in 2008. Remuneration of the principal staff hours was postponed until then and pending approval of the present final report.

- In September 2008, theoretical work on QoS support in noncooperative ad hoc WLAN settings with anonymous stations and on a related topic of distributed reputation systems was finished; the results were discussed with the Consultant and presented in part at the beginning of the following month by the PI and a co-worker at the 5th Polish-German Teletraffic Symposium (PGTS 2008) in Berlin.

- During the same meeting, final consultation regarding the first phase of the project took place between the PI and Consultant in the form of a series of extensive discussions concluded with delimiting the work to be included in the present final report and outlining the

issues to be submitted within a follow-up proposal, a possibility indicated by the Project Manager in preliminary talks in the autumn of 2007.

- In November and December 2008, theoretical results of research on QoS support in non-cooperative wireless settings were presented by the PI at two conferences with proceedings to be made available online in the IEEE Xplore database, namely IFIP Wireless Days (WD 2008) at Dubai, UAE, and the above mentioned 5th International Conference on Innovations in Information Technology (Innovations'08) at Al Ain, UAE.

- In November 2008, an agreement was reached between the PI and the Gdansk University of Technology, Poland, authorities whereby the period of performance of the project was extended until March 2009, in order to formally enable remuneration originating from the final installment of the funding, in the case the December 2008 report was approved by the EOARD.

- In February 2009, the last $30,268 installment of the project's first phase was received and the check was cashed about five weeks later. It was used to remunerate the principal staff hours and to reimburse the travel expenses related to the Innovations'08 conference that had been temporarily funded from a local grant.

- In May and September 2009, during his two visits at Gdansk University of Technology, the Consultant discussed the project status and forthcoming activities with the PI, in particular to explore the possibility of incorporating more refined models of information percolation through an ad hoc network topology; these are considered to be included in the journal versions being prepared as follow-ups of selected conference papers produced within the project.

- In August 2009, Dr. Kevin Kwiat of Air Force Labs in Rome NY visited Gdansk to learn the project's current status and results; these were presented during a 2-hour seminar and followed by submission of a slide presentation as a basis for a current status report.

- Between September and December 2009, selected results of the project were presented by the PI and a co-worker at the following international conferences: 2nd IEEE Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2009) at Bratislava, Slovakia; 16th Polish Teletraffic Symposium 2009 at Lodz, Poland; IFIP WG 6.8 Joint Conference on Wireless and Mobile Networking (WMNC 2009) at Gdansk, Poland; IFIP Wireless Days 2009 at Paris, France; ACM Modeling and Simulation of Wireless and Mobile Systems (MSWiM 2009) at Tenerife, Spain, and IEEE Int. Conf. on New Technologies, Mobility and Security (NTMS'09) at Cairo, Egypt.

- In January 2010, a $35,268 installment of the project's second phase was received and the check was cashed in the following month. It was partly used to remunerate the principal staff hours, the remaining sum (and the last installment expected if this report is approved) being held in reserve for final staff hours remunerations and possible conference expenses at the end of 2010.

- In April 2010, the PI took part as TPC vice-chair in a workshop on survivability in cyberspace, organized by Dr. Kwiat as part of CPSWeek conference in Stockholm. During that visit, funded in part by the AFOSR from a separate appropriation, the PI and Dr. Kwiat discussed the current developments within the project as well as the directions of future cooperation.

- In May 2010, the PI reached an agreement with Gdansk University of Technology authorities as to an extension of the project performance period in the local files, so as to enable making payments from the present and final funding after the contract end date of June 14, 2010. Also, the project final phase was discussed with the Consultant during his visit to Gdansk.

- In June 2010, further results of the project were presented at the IEEE HotMesh workshop at Montreal, Canada, and 2nd IEEE Conference on Information Technology at Gdansk, Poland. During the HotMesh event, another discussion with Dr. Kwiat took place, whose purpose was to plan future collaboration on game-theoretic analyses of defense mechanisms against malicious and selfish behavior in multihop wireless networks.

Meanwhile, the Consultant and his collaborators continued their work on information-theoretic aspects of data flow across wireless network structures, with the emphasis on selection and calculation of appropriate measures of information and the speed of information transfer through ad hoc environments. The results were presented at a number of conferences and published in several scientific journals throughout the period between 2007 and 2010; part of the findings, including joint work with the PI, were presented by the Consultant during his invited talk at the October 2008 PGTS symposium, as well as at a May 2010 special session at Gdansk University of Technology.

2. Summary of technical results

The project's noncooperative behavior in wireless networks track uses analytical, simulative as well as experimental techniques. It is especially important in ad hoc networks, where administrative enforcement of cooperative behavior of the network stations is not possible. Although still regarded as a partly unfulfilled dream, ad hoc, mesh, and other unstructured networks are worth studying due to their potential of becoming an alternative communication infrastructure in the cases of major disasters or security breaches. Our research regarding medium access control (MAC) protocols in a noncooperative wireless local-area network (WLAN) environment assumes that each station strives to maximize its own throughput- and energy-related payoff. Analysis of noncooperative behavior calls for a game-theoretic approach, since upon configuring its MAC protocol autonomously, a station experiences a payoff dependent on other stations' configurations, but cannot regard any form of inter-station contracts or alliances as binding, hence enters a noncooperative *MAC game*. Analytical payoff model being used is an extension of Bianchi's Markovian approximation of a WLAN under saturation, previously developed under Grant FA8655-04-1-3074 in order to study aggressive backoff configuration and long-term station strategies forming a subgame perfect Nash equlibrium of repeated MAC games. Some simulative and experimental confirmation, as well as quantitative corrections of the resulting bandwidth distribution among the stations, was obtained in Gdansk University of Technology's local lab environments [1].

If a set of strategies is allowed for each station, ranging from aggressive to cooperative (as measured by the persistence of transmission attempts at the price of increased energy expenditure) then we conclude that the payoff structure of such a MAC game coincides with that of a multiperson Prisoners' Dilemma on condition that attention is restricted to the *contention region* (the only one of practical importance, where a station's throughput increases in the probability of a successful transmission attempt). We find that the above characterization justifies a reduction of the game to a two-strategy case (aggressive vs. cooperative, with intermediate strategies removed). Let $b_c(N, j)$ ($N \geq j$) and $b_a(j)$ ($j > 0$) denote a cooperative and aggressive

station's throughput, respectively, with N stations, of which j are aggressive. We anticipate the following payoff structure: $b_a(j)$ decreases with j; for any N, $b_c(N, 0)$ decreases with N, $b_c(N, j) \approx 0$ for $j > 0$ (which is why $b_c(j)$ does not depend on N), $b_a(j + 1) > b_c(N, j)$, and $b_c(N, 0) > b_a(N)$. Adding a third plausible strategy, called *greedy* (consisting in the disengagement of the backoff scheme), complicates the incentive structure of the game. This is investigated in [2].

QoS sensitivity of WLAN stations' traffic may be expressed by a requirement of a minimum throughput R. Being granted less upon a request for data transfer, a station perceives its payoff as zero. This is a significant modification of the MAC game payoff structure, hence we use the term *QoS game*. In a cooperative distributed environment, some "social goals" can be achieved: QoS is allocated *fairly* (thanks to the symmetry of the request acquisition mechanism underlying MAC protocols), *efficiently* (thanks to MAC design optimizations) and *firmly* (meaning that once allocated, QoS is maintained throughout the whole data transfer regardless of subsequent requests, as guaranteed by appropriate admission mechanisms). However, in a noncooperative environment, WLAN station are only interested in their individual payoffs and not in any "social goals". Again reducing the game to the two-strategy (aggressive vs. cooperative) case, we consider an asynchronous move version of McCain's "FIFO game", with the stations switching between their cooperative and aggressive strategies until few enough play aggressive so that the R requirement is met (these stations are the winners). Henceforth, switching from cooperative to aggressive by the other stations is non-Nash and data transfer can start without violation of firmness. A game-theoretic approach based on stochastic games, with the corresponding solution concept of Markov perfect equilibrium, is the subject of [3]. Drawing upon an earlier paper within our previous Grant FA8655-07-1-3071 work, this paper states in a more precise way the derivation and location of the Markov perfect equilibria in relation to a station’s power budget. The danger of too high a power budget is visible in the Markov perfect equilibria almost coinciding with the “valleys” in an efficiency vs. station strategy plots. Another two-strategy (greedy vs. cooperative) case calling for a Bayesian game approach, with the corresponding solution concept of symmetric Bayesian equilibrium, is presented in [4]. Locating these equilibria and evaluating the resulting bandwidth utilization are the main results; the research concludes that despite the anonymous noncooperative ad hoc setting, fairness, efficiency and firmness can still be achieved using self-regulatory (rather than administrative) mechanisms. To this end, redefining channel contention at session (rather than frame) level is necessary, leading to auction-like contention. The presented approach was somewhat incomplete, yet was recognized as a promising area of further research, since it can deal with various kinds of selfish attacks based on manipulating a station’s identity, and allows for the worst case of “3S” (selfish, secretive, and short-sighted) stations, a model never treated before in a formal way. The paper [5], whose preliminary version was presented at a national computer networking forum [6] develops these ideas further, with a more systematic analysis, simulations of dynamic game scenarios, and reflection upon a new type of attack called “post-bidding load”. A particularly attractive feature of the model is that “post-bidding load” can be analyzed with a single differential equation. Moreover, simple but effective means of neutralizing a multiple identity attack can be devised. A journal version of the paper is under preparation.

Besides single-channel WLANs, the developed payoff models permit to analyze interaction of intelligent selfish wireless stations selecting among multiple wireless network services (and technologies) available in the geographic area they roam. A generic wireless station is equipped in a set of transceivers enabling it to access a number of networks, possibly heterogeneous in terms of PHY-layer data rates and access protocols, and to flit from one to another whenever it may improve its short-term transmission characteristics. Of special interest is a

situation when the station can only access one network at a time; in this case the term *wireless multihoming* is used, analogous to site multihoming implemented by several interfaces connected to different Internet service providers. In classical design, the station collects feedback on available transmission quality from each network it can connect to and makes an optimal decision. The need for a game-theoretic analysis arise when the feedback cannot keep pace with the time-varying traffic and propagation conditions, or the multihomed stations are free to reselect a network in response to other stations' selections. In both cases the stations find themselves in a noncooperative one-shot game (where a player does not know other players' actions before taking its own). We refer to the resulting game as *wireless multihoming game* and analyze the payoff (i.e., the long-term average received bandwidth share) distribution it produces among a set of stations. Of the possible control variables a station can self-optimize in pursuit of a high payoff, such as PHY-layer rate, transmission power, network selection, and MAC protocol configuration, our analysis focuses on the latter two; note that aggressive MAC protocol configuration typically corresponds to increased transmission power expenditure. Although in the literature wireless multihoming scenarios have been modeled as (analytically attractive) population games, the use of evolutionary game theory being justified by assuming a large number of stations, we find an individualistic approach more suitable and practical. The reason is that at any given time, the number of stations saturated with source traffic is likely to be on order of a dozen or a few dozens rather than thousands or more. Studies of wireless multihoming games have so far been confined to selfish network selection (in which case they resemble the well-known minority game and often are considered as channel assignment-type potential games) or selfish MAC protocol configuration (described above in the context of a single WLAN, where a multiplayer Prisoners' Dilemma arises). A wireless multihoming game where a station can selfishly control both the network selection and MAC protocol configuration (i.e., exhibits "2D selfishness") is a new quality missing in current literature and worth studying.

In [7] an attempt is made to model a wireless multihoming game as a two-action one, where each station can select between the Honest and Selfish modes of operation. In the former, the MAC protocol is configured according to the IEEE 802.11 standard and networks are selected at random using a uniform probability distribution; in the latter, the backoff mechanism is selfishly manipulated and the network selection probability distribution is strongly tilted towards available high-speed WLANs. We discuss the existence and location of pure and mixed symmetric Nash equilibria of the game (at present, we can prove that with the backoff mechanism, the latter is unique), as well as outline a method of detection of the number of stations in the Selfish mode despite their anonymity. Later, this method is exploited by an idea bag-type dynamic strategy, inspired by the experience with the minority game, that switches between the two modes of operation in a manner similar to that described in a different context by an earlier paper within our previous Grant FA8655-07-1-3071. The two-action game model is next applied in [8] with the aim of calculating and evaluating the game's correlated equilibrium, a concept that has been used in very few existing papers on wireless networking and that promises increased payoffs to all the stations without violating their decisive autonomy (i.e., not imposing centralized control in any form). Comparisons with mixed Nash equilibrium play are made from the viewpoint of several plausible requirements as to the payoff distribution. Finally, in a recent paper [9] we have calculated in a closed form the symmetric mixed Nash equilibrium in a wireless multihoming game with "2D selfishness" and demonstrated the resulting bandwidth distribution to be inferior to all-honest play. Thus a more realistic "capacity" of a multi-WLAN system with autonomous rational stations has been determined. While aggressive MAC protocol configuration unsurprisingly turns out to dominate standard MAC protocol configuration, there seems to be a way to employ a grim trigger-like

retaliation strategy so as to disincentivize disengaging backoff by multiple stations accessing the same WLAN at a given time. Moreover, distributed public randomization schemes supporting a correlated Nash equilibrium seem possible and preliminary work on them has already been started. We think this direction of research is quite promising and we hope to follow through. Another way of viewing the problem leads to a channel assignment game where a selfish station's objective is to minimize the number of aggressive (more power-consuming) MAC configurations in the available channels subject to the minimum bandwidth required for a certain level of QoS support; earlier work on QoS games in a single WLAN might be drawn upon. It is expected that further research along these lines will contribute to the rapidly emerging field of cognitive radio design.

The investigation of the upshot of, and ways to protect against, selfish MAC-layer behavior in single- or multi-WLAN scenarios should be accompanied by a discussion of cooperative security at the network and transport layers. The paper [10] discusses the need for a fully-distributed reputation system dedicated for multihop wireless ad hoc networks whose stations may exhibit selfish forwarding (network-layer) behavior. A reputation-based system is proposed that retains anonymous packet forwarding and featuring a congestion avoidance mechanism. In [11], we focus on selfish configuration of the TCP (transport-layer) congestion avoidance mechanism that can lead to aggressive usage of network resources by some packet flows at the cost of other flows. Of interest is the quantitative impact of selfish TCP configuration in large networks with multiple bottlenecks, which we regard as typical of future large-scale ad hoc topologies. Both these lines of research i.e., reputation systems-based and transport layer parameters reconfiguration-based, hold promise for a more integrated approach to cooperative security at the transport layer. In the former, a logical step is to replace watchdog-like local mechanisms of gathering first-hand behavioral information by end-to-end transaction-oriented ones, and to employ a more systematic rule of combining behavioral information from different sources; this was elaborated upon in a few papers described below. The latter avenue of research should produce interesting results especially for wireless network-oriented versions of TCP.

A reputation system serves to detect selfish stations in regard to a specific function e.g., packet routing or forwarding (a companion scheme of punishing or ostracizing selfish stations is beyond the scope of this project). The papers [12–15] aim at overcoming some principal drawbacks of most currently existing reputation systems in wireless networks in regard to forwarding, such as employment of the unreliable low-layer watchdog mechanism for gathering first-hand behavioral information (which obliges a station to promiscuously overhear transmissions by its neighbor stations, and is tied to specific MAC-layer protocols), or vulnerability to various malicious attacks. To dispense with the watchdog, we delegate the distinction between apparent and real selfish behavior to separate mechanisms and advocate a more flexible approach of end-to-end session-level acknowledgments. The proposed DST-SDF approach [12–14] has each source station of a packet flow form, and receive as second-hand behavioral information, only yes-or-no recommendations regarding whole source-to-destination routes rather than particular on-route stations. Individual stations' reputation metrics are then derived using simple heuristics. Dempster-Shafer theory of evidence (DST) is used to deal with conflicting recommendations received from different stations without assuming artificial Bayesian priors; a systematic way of using DST to integrate recommender trust building (credibility of a recommending station) into trust building in regard to forwarding is described in [15]. Trustworthiness of exchanged recommendation reports is solely based on their contents and recommending stations' location. Simulative experiments have confirmed that the proposed system is robust against malicious false recommendations (albeit

only consisting in a reversal of content in a recommendation report being forwarded), while ensuring relatively fast convergence i.e., detecting all selfish nodes in the network within a reasonable time.

In order to hide its selfish routing or forwarding behavior, a wireless station has to manifest it in a restrained way i.e., forward or route packets at times. Our recent research into reputation systems was to answer the question what tradeoff between the risk of being detected and the power expense necessary to imitate honest behavior a selfish station faces. In [16] we conducted a preliminary study in the absence of malicious stations i.e., without any provisions for false accusation attacks (fake reports implying selfish behavior of other stations), and assuming that the selfish stations launch a selective session drop-type attack. We found via simulation that a route-based reputation metric incremented uniformly for all on-route stations upon lack of a session-level acknowledgment creates a clear Pareto frontier for selfish stations in the detection risk vs. power expense plane. However, the corresponding tradeoff is in large part relaxed if the selfish stations launch a false appreciation attack (fake reports implying own honest behavior). Contrary to the prevailing opinion that selfishness in resource sharing systems brings about a tragedy of the commons, the tradeoff becomes more favorable to the selfish stations if they grow in numbers. We are now working on two possible solutions, one involving a modification of the reputation metric, and the other involving a distributed revocation scheme. Another question that arises is whether selfish forwarding or routing behavior is beneficial if a station's power expense is unlimited (as is the case e.g., in wireless mesh networks, whose wireless routers are connected to the mains electricity supply), hence the only motivation left is related to the bandwidth a station can save for its own source traffic by refusing to relay transit traffic. In [17] we have conducted an extensive simulation study under DSR routing to find that scenarios where a selfish station can benefit are few; currently we are following up on this and look for suitable modifications of DSR to discourage selfish behavior altogether in wireless mesh environments.

Within the project's information-theoretic track, in order to appreciate the effects of withholding control information, we studied in a number of papers the various aspects of information transfer, both in its generality and in specific environments such as wireless networks. In [18], and subsequently in [30] and [31], we proposed a general definition of information and identified four unexplored aspects of information, namely semantic information, spatial and temporal information, and structural information. We also realized that information and computation are closely related. In [30] we also discussed the speed of information in wireless ad hoc networks when users are initially disconnected. This is the first step towards understanding spatio-temporal capacity of such networks. Finally, we discussed the value of information in the network context using game theoretic methodology. To evaluate the impact of noncooperative station behavior we need a reference network capacity estimate taking into account the context C of information and the application-level protocol P of retrieving it at the stations. A meaningful definition of information, unlike Shannon's, should therefore reflect its semantic aspects and the capabilities of its recipients. We have been experimenting with measures of information within the so-called event-driven paradigm. Preliminary considerations based on the entry deterrence model are presented in [18]; they aim at quantifying the reduction of information transfer capabilities due to the stations' noncooperative behavior and lack of mutual trust. This topic is to be explored further. In the forthcoming paper [31] we plan to discuss "learnable information" and spatio-temporal aspect of information in wireless and ad hoc networks.

In [19–27], and [28–36] we deal with other specific aspects of information. For example, in [19] an error resilient Lempel-Ziv'77 scheme has been designed that also can be used for information hiding. In [23] and [33] we propose a precise analysis of variable-to-variable code that achieves very small redundancy. This was thoroughly discussed in our invited paper [28]. The proof technique is also novel: we used theory of sequences module 1 and Diophantine approximations. In [21], [27], and [32] we considered constrained coding and analyze the number of pattern occurrences in constrained coding. In our previous papers we estimated the entropy of a hidden Markov model (a long standing open problem), and used it in [20] and [28] to obtain for the first time an asymptotic expansion of the noisy constrained capacity for small noise. Finally, in [25] we looked at source coding beyond prefix codes and established mini-max redundancy for such codes, perhaps leading to an ultimate bound for universal redundancy. In [34] and [35] we believe we made the first step towards understanding information embodied in structures.

Information theory traditionally deals with "conventional data," be it textual, image, or video data. However, databases of various sorts have come into existence in recent years for storing "unconventional data" including biological data, social data, web data, topographical maps, and medical data. In compressing such data, one must consider two types of information: the information conveyed by the structure itself, and the information conveyed by the data labels implanted in the structure. In [34] we attempt to address the former problem by studying information of graphical structures (i.e., unlabeled graphs) while in [35] we discussed the structural complexity of random binary trees. All of these papers can be viewed as an attempt to go beyond Shannon and provide adequate formalism for extraction, comprehension, and manipulation of information in scientific and social domains leading to a new science of information. We have recently launched the Institute for Science of Information and started the NSF STC Center for Science of Information to address these issues.

Compared with our original plans outlined in the project proposal, there remain two topics we have not been able to study in detail, namely agreed delivery multicast and P2P transfer related issues in a game- and information-theoretic framework. We had hoped to include them into the extended timeframe of the project (current end date is June 14, 2010). In the course of the project, we decided to shift the emphasis as described above for three reasons. First, our research into WLAN and multi-WLAN models seems to have produced a number of interesting results, in fact even more than we had expected, which we felt deserved expanding upon instead of opening new lines of research. Second, the prime objective of including agreed order multicast and cooperation in P2P overlays was to reflect selfish behavior in multihop wireless topologies; as the project evolved, this was in our opinion better addressed through the investigation of reputation and selfishness effects in MANET and mesh environments, as documented above. Finally, it seems in retrospect that agreed order multicast and cooperation in P2P overlays would have considerably enlarged the scope of our research, limited by the human resource at our disposal. We feel that when placed in a more comprehensive context of cooperative security, they justify a separate track in a future project if one is initiated.

Attached to this report are pdf files of the papers listed below except [31], which is still under preparation and currently only available as a fragmented manuscript (however, will acknowledge the funding under the present grant when published). Please note that [2], [20], [21], [24], [25], and [27] were published shortly after the commencement of the project before its number was changed, therefore acknowledge the funding under the original grant number FA8655-07-1-3071. Finally, [19], [22], and [26] are recent enhanced versions of publications

using some results and approaches developed within the former Grant FA8655-04-1-3074, and therefore acknowledge the funding under that grant number.

Paper list

1. K. Gierlowski, T. Gierszewski and J. Konorski, *Distributed Protection against Non-cooperative Node Behavior in Multi-hop Wireless Networks*, Proc. 1st IEEE Int. Conf. on Information Technology, Gdansk, Poland, May 2008, pp. 61-64, IEEE Xplore, DOI = 10.1109/INFTECH. 2008.4621591.
2. J. Konorski, *IEEE 802.11 LAN Capacity: Incentives and Incentive Learning*, Systems Science, vol. 33, No. 4, 2007, pp.111-118.
3. J. Konorski, *Noncooperative QoS Support in an Ad Hoc WLAN*, Proc. IFIP Wireless Days 2008, Dubai, UAE, Nov. 2008, IEEE Xplore DOI = 10.1109/WD.2008.4812857.
4. J. Konorski, *QoS Provision in an Ad Hoc IEEE 802.11 WLAN: A Bayesian War of Attrition Model*, Proc. 5th Int. Conf. Innovations in Information Technology, Al Ain, UAE, IEEE Xplore, DOI = 10.1109/INNOVATIONS. 2008.4781686.
5. J. Konorski, *Ad Hoc WLAN with Selfish, Secretive, and Short-Sighted Stations*, Proc. 2nd Int. Symp. on Applied Sciences in Biomedical and Comm. Technologies ISABEL 2009, Bratislava, Slovakia, Nov. 2009, IEEE Xplore DOI = 10.1109/ ISABEL.2009.5373650
6. J. Konorski, *Wireless LAN with Noncooperative Anonymous Stations: QoS provisioning Via War of Attrition*, Proc. 16th Polish Teletraffic Symposium 2009, Łodz, Poland, Sept. 2009, s. 87-90
7. J. Konorski, *Wireless Multihoming Modeled as a Multi-WLAN Game*, Proc. ACM MSWiM 2009, Tenerife, Spain, Oct. 2009, ACM Press, 2009, pp. 147-154
8. J. Konorski, *Ad Hoc Multi-WLAN: A Game-Theoretic Model of Correlated Play*, Proc. IFIP Wireless Days 2009, Paris, Dec. 2009, IEEE Xplore DOI = 10.1109/WD.2009.5449693
9. J. Konorski, *Equilibria of a Wireless Multihoming Game*, Proc. 2nd Int. IEEE Conf. on Information Technology, Gdansk, Poland, June 2010, to appear in IEEE Xplore 2010
10. J. Konorski and R. Orlikowski, *Distributed Reputation System for Multihop Mobile Ad Hoc Networks*, Proc. 5th Polish-German Teletraffic Symposium PGTS 2008, Berlin, Oct. 2008, pp. 161-167.
11. J. Konorski and J. Lis, *Testing Aggressive TCP Configurations*, Proc. 1st IEEE Int. Conf. on Information Technology, Gdańsk, Poland, May 2008, pp. 81-84, IEEE Xplore, DOI = 10.1109/ INFTECH.2008.4621596.
12. J. Konorski, R. Orlikowski: *DST-Based Detection of Non-cooperative Forwarding Behavior of MANET and WSN Nodes*, Proc. IFIP WG 6.8 Joint Conference, WMNC 2009, Gdansk, Poland, Sept. 2009, vol. AICT 308, Springer-Verlag 2009, pp. 185-196.
13. J. Konorski, R. Orlikowski: *Dempster-Shafer Theory-Based Trust and Selfishness Evaluation in Mobile Ad Hoc Networks*, Proc. 16th Polish Teletraffic Symposium 2009, Lodz, Poland, Sept. 2009, pp. 91-94.
14. J. Konorski, R. Orlikowski: *A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks*, J. Telecomm. Inform. Technology, 2, 2009, pp. 30-34.

15. J. Konorski, R. Orlikowski: *Data-Centric Dempster-Shafer Theory-Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs*, Proc. 3rd IEEE Int. Conf. on New Technologies, Mobility and Security NTMS'09, Cairo, Egypt, Dec. 2009, IEEE Xplore DOI = 10.1109/NTMS.2009.5384817.
16. J. Konorski, *Selfishness Detection in Mobile Ad Hoc Networks: How Dissemination of Indirect Information Turns into a Strategic Issue*, Proc. 2nd Int. IEEE Conf. on Information Technology, Gdansk, Poland, June 2010, to appear in IEEE Xplore 2010.
17. K. Gierłowski, J. Konorski, *Router Selfishness in Community Wireless Mesh Networks: Cross-Layer Benefits and Harms*, Proc. IEEE HotMesh 2010, Montreal, Canada, June 2010, to appear in IEEE Xplore 2010.
18. J. Konorski and W. Szpankowski, *What is Information?*, Festschrift in Honor of Jorma Rissanen, Tampere, Finland, TICSP Series #38, 2008, pp.154-172; short version published in Proc. IEEE Information Theory Workshop 2008 (ITW '08), May 2008 pp. 269 – 270, IEEE Xplore DOI = 10.1109/ITW. 2008.4578666.
19. S. Lonardi, W. Szpankowski and M. Ward, *Error Resilient LZ'77 Data Compression: Algorithms, Analysis, and Experiments*, IEEE Trans. Information Theory, 53, 1799-1813, 2007.
20. P. Jacquet, G. Seroussi and W. Szpankowski, *Noisy Constrained Capacity*, 2007 International Symposium on Information Theory, 986-990, Nice, France, 2007.
21. Y-W. Choi and W. Szpankowski, *Pattern Matching in Constrained Sequences*, 2007 International Symposium on Information Theory, 2606-2610, Nice, France, 2007.
22. L. Devroye, G. Lugosi, G. Park, and W. Szpankowski, *Multiple Choice Tries*, *Random Structures & Algorithms*, 32, 2008; IEEE Xplore, DOI = 10.1002/rsa.20234.
23. Y. Bugeaud, M. Drmota, and W. Szpankowski, *On the Construction of (Explicit) Khodak's Code and Its Analysis*, IEEE Trans. Information Theory, 54, 5073-5086, 2008.
24. G. Pandurangan and W. Szpankowski, *A Universal Caching Algorithm Based on Pattern Matching*, Algorithmica, 2008 IEEE Xplore, DOI = 10.1007/s00453-008-9196-9.
25. W. Szpankowski, *A One-to-One Code and Its Anti-redundancy*, IEEE Trans. Information Theory, 54, 4762-4766, 2008.
26. G. Park, H-K. Hwang, P. Nicodeme, and W. Szpankowski, *Profile of Tries*, SIAM J. Computing, 2009; also Proc. LATIN'08, LNCS 4957, 1-11, 2008.
27. Y.W. Choi and W. Szpankowski, *Large Deviations for Constrained Pattern Matching*, Proc. ISIT'08, Toronto, 2141-2145, 2008.
28. W. Szpankowski, *Average Redundancy for Known Sources: Ubiquitous Trees in Source Coding*, Proc. Fifth Colloquium on Mathematics and Computer Science Algorithms, Trees, Combinatorics and Probabilities, 19–58, September 22-26, Blaubeuren, Germany, 2008.
29. M. Drmota and W. Szpankowski, *(Un)Expected Behavior of Digital Search Tree Profile*, Proc. SODA 2009, New York, 2009.
30. W. Szpankowski, *Facets of Information in Communications*, Proc. 5-th Polish-German Teletraffic Symposium, 5-14, Berlin, Oct. 2008.
31. J. Konorski and W. Szpankowski, *Facets of Information*, in preparation.

32. Y. Choi and W. Szpankowski, *Constrained Pattern Matching*, ACM Trans. Algorithms, 2010 (to appear).

33. M. Drmota, Y. Reznik, and W. Szpankowski, *Tunstall Code, Khodak Variations, and Random Walks*, IEEE Trans. Information Theory, 56, 2928 - 2937, 2010.

34. Y. Choi and W. Szpankowski, *Compression of Graphical Structures*, Proc. 2009 International Symposium on Information Theory, 364-368, Seoul, 2009.

35. J. Kieffer, E-H. Yang, and W. Szpankowski, *Structural Complexity of Random Binary Trees*, Proc. 2009 International Symposium on Information Theory, 635-639, Seoul, 2009.

36. W. Szpankowski and S. Verdu, *Minimum Expected Length of Lossless Compression of Memoryless Sources*, Proc. 2009 International Symposium on Information Theory, 369-373, Seoul, 2009.